

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年12月25日
Date of Application:

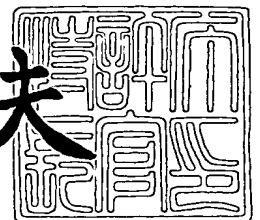
出願番号 特願2002-374721
Application Number:
[ST. 10/C]: [JP 2002-374721]

出願人 カシオ計算機株式会社
Applicant(s):

2003年11月 6日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3091761

【書類名】 特許願

【整理番号】 02-1507-00

【提出日】 平成14年12月25日

【あて先】 特許庁長官 殿

【国際特許分類】 G06T 1/00
G06K 9/00

【発明者】

【住所又は居所】 東京都羽村市栄町 3 丁目 2 番 1 号 カシオ計算機株式会
社 羽村技術センター内

【氏名】 喜多 一記

【特許出願人】

【識別番号】 000001443

【氏名又は名称】 カシオ計算機株式会社

【代理人】

【識別番号】 100090033

【弁理士】

【氏名又は名称】 荒船 博司

【選任した代理人】

【識別番号】 100093045

【弁理士】

【氏名又は名称】 荒船 良男

【手数料の表示】

【予納台帳番号】 027188

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 カード型デバイスおよび認証システム

【特許請求の範囲】

【請求項 1】 電子機器と接続端子を介して接続されるカード型デバイスであって、

接続端子を有するカード型の筐体と、

この筐体の端面にその外周面が突出して設けられた回転ローラと、

この回転ローラの外周面に当接される指の一次元指紋データを取得する一次元指紋データ取得部と、

前記回転ローラを回転させることにより、前記一次元指紋データ取得部により位置を連続的に変えて取得される一次元指紋データから二次元像としての指紋データを合成する指紋データ合成部と、

前記電子機器との間でデータの授受を行うインターフェース部と、

を備えたことを特徴とするカード型デバイス。

【請求項 2】 請求項 1 に記載のカード型デバイスにおいて、

前記筐体は、前記接続端子が配されるとともに前記電子機器に設けられたカード・スロットに挿入される挿入部を備え、前記回転ローラはこのカード・スロットの挿入口から露出する端面に設けられることを特徴とするカード型デバイス。

【請求項 3】 請求項 1 または 2 に記載のカード型デバイスにおいて、

前記指紋データを、当該カード型デバイスに固有であり、かつ、対となる公開復号鍵によってのみ復号化することができる秘密暗号鍵により暗号化する暗号化手段を備えたことを特徴とするカード型デバイス。

【請求項 4】 請求項 1 または 2 に記載のカード型デバイスにおいて、

前記指紋データ合成部により合成された指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、前記インターフェース部における前記電子機器との間のデータの授受を制限する制御部を備えたことを特徴とするカード型デバイス。

【請求項 5】 電子機器と、請求項 1 または 2 に記載のカード型デバイスとが接続されてなる認証システムであって、

前記電子機器は、前記カード型デバイスから送信される指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、当該電子機器の動作を制限する制御部を備えたことを特徴とする認証システム。

【請求項 6】 電子機器と、請求項 3 に記載のカード型デバイスとが接続されてなる認証システムであって、

前記電子機器は、前記カード型デバイスから送信される暗号化された指紋データを前記公開復号鍵により復号化し、復号化された指紋データと予め登録された指紋データとの一致を照合し、両指紋データが一致しない判断した場合、当該電子機器の動作を制限する制御部を備えたことを特徴とする認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、カード型デバイスおよび認証システムに関する。

【0002】

【従来の技術】

近年、電子機器のネットワーク化が進み、電子機器間の通信が自由になり、どこからでも様々な情報にアクセスできるようになってきている。それに伴い他者の不正アクセスを防止するためにセキュリティの重要性が高まっている。セキュリティ技術の一つに指紋によってユーザを認証する方法があり、指紋読取センサを P C カードに設けたものがある。

【0003】

例えば、C C D (Couple charged Device) 等から成る指紋読取センサを P C カードの把持位置に設けたものがある (特許文献 1 参照)。この P C カードを把持すると、自動的に指紋が採取され、指紋に基づいて使用者の認証が行われ、P C カードに記憶された個人情報等へのアクセスが防止されるようになっている。

【0004】

他の例として、P C カードの挿入部に指紋読取センサを備えた指紋読取センサを相対回転可能に機械的に連結したものもある (例えば、特許文献 2 参照)。

この P C カードを電子機器のカード・スロットに装着させることにより、本人

を認証するための認証装置として使用することができ、認証されない場合は電子機器の動作が制限されたり、PCカードへのアクセスが禁止される。

【0005】

【特許文献1】

特開 2000-48177 号公報

【特許文献2】

特開 2001-233344 号公報

【0006】

【発明が解決しようとする課題】

しかしながら、特許文献1に記載の指紋読取センサは把持位置に設けられているので、PCカードを電子機器のカード・スロットに装着すると指紋読取センサがカード・スロットの内部に配されてしまい、PCカードを電子機器に装着した状態でユーザを認証することはできなかった。

一方、特許文献2に記載の指紋読取センサは、PCカードを電子機器のPCカードスロットに装着させたときに大きく外部へ突出してしまうので、この指紋読取センサ付きのPCカードを電子機器に装着させたままで携帯させにくいという問題があった。

【0007】

また、両指紋読取センサは、指を載置可能な平面矩形状に形成されており、CCDなどの高価な半導体素子を用いるためコスト高となる。さらに、二次元CCDチップは実装面積を要することから、携帯電話やPDA(Personal Digital Assistance)等の拡張メモリとして使用されるCFカード(Compact Flash Card)、SDカード(Secure Digital Card)、MMC(Multi Media Card)カード、USB接続携帯型フラッシュメモリ等の超小型のメモリカードに指紋読取センサを設けることはできなかった。このため、指紋認証によりこれらのメモリカードに記憶された情報を保護したり、携帯電話やPDA等にメモリカード等により指紋認証機能を拡張させることができなかった。

【0008】

本発明の課題は、指紋読取センサを搭載した超小型のカード型デバイスおよび

このカード型デバイスを用いた認証システムを提供することである。

【0009】

【課題を解決するための手段】

上記課題を解決するために、請求項1に記載の発明は、電子機器と接続端子を介して接続されるカード型デバイスであって、接続端子を有するカード型の筐体と、この筐体の端面にその外周面が突出して設けられた回転ローラと、この回転ローラの外周面に当接される指の一次元指紋データを取得する一次元指紋データ取得部と、前記回転ローラを回転させることにより、前記一次元指紋データ取得部により位置を連続的に変えて取得される一次元指紋データから二次元像としての指紋データを合成する指紋データ合成部と、前記電子機器との間でデータの授受を行うインターフェース部と、を備えたことを特徴とする。

【0010】

請求項1に記載の発明によれば、一次元指紋読取センサにより指紋の二次元像を得ることとしたので、指紋読取センサを実装するための面積も小さくすることができ、CFカード等の超小型のメモリカードにも指紋読取センサ設けることができる。また、二次元の指紋読取センサを設ける場合に比べて、指紋センサを構成する部品コストを低減することができる。これらにより、携帯電話やPDA等の一般ユーザ向けの携帯用電子機器にも容易に指紋認証機能を拡張させることができる。

【0011】

さらに指を回転ローラに当接させた状態で回転させることにより、指を一次元指紋読取センサに対して移動させることができるので、指の変形やゆがみを防止した状態で一次元指紋読取センサに指紋を読み取らせることができ、操作性に優れている。

【0012】

請求項2に記載の発明は、請求項1に記載のカード型デバイスにおいて、前記筐体は、前記接続端子が配されるとともに前記電子機器に設けられたカード・スロットに挿入される挿入部を備え、前記回転ローラはこのカード・スロットの挿入口から露出する端面に設けられることを特徴とする。

【0013】

請求項2に記載の発明によれば、回転ローラはカード・スロットの挿入口から露出する端面に設けられるので、カード型デバイスを装着させた状態でカード・スロットから指紋読取センサが大きく突出することがなく、携帯性に優れている。また、ユーザは、カード・スロットの挿入口に直交するように指をスライドさせればよいので、操作性に優れている。

【0014】

請求項3に記載の発明は、請求項1または2に記載のカード型デバイスにおいて、前記指紋データを、当該カード型デバイスに固有であり、かつ、対となる公開復号鍵によってのみ復号化することができる秘密暗号鍵により暗号化する暗号化手段を備えたことを特徴とする。

【0015】

請求項3に記載の発明によれば、暗号化手段により指紋データを秘密暗号鍵により暗号化するので、暗号化された指紋データはこの秘密暗号鍵と対となる公開復号鍵を有するものにしか復号化することができず、指紋データの悪用を防ぎ、セキュリティをより高めることができる。

【0016】

請求項4に記載の発明は、請求項1または2に記載のカード型デバイスにおいて、前記指紋データ合成部により合成された指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、前記インターフェース部における前記電子機器との間のデータの授受を制限する制御部を備えたことを特徴とする。

【0017】

請求項4に記載の発明によれば、カード型デバイスを電子機器に接続する前に指紋に基づいてユーザを認証することできる。また、一次元指紋読取センサを介して取得された指紋データが、予め登録された指紋データと一致しない場合は、電子機器との間のデータの授受が制限されるので、カード型デバイスの不正使用およびカード型デバイスへの不正アクセスを防止することができる。

【0018】

請求項 5 に記載の発明は、電子機器と、請求項 1 または 2 に記載のカード型デバイスとが接続されてなる認証システムであって、前記電子機器は、前記カード型デバイスから送信される指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、当該電子機器の動作を制限する制御部を備えたことを特徴とする。

【0019】

請求項 5 に記載の発明によれば、電子機器はカード型デバイスから送信される指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、制御部は電子機器の動作を制限するので、電子機器およびカード型デバイスの不正使用およびカード型デバイスへの不正アクセスを防止することができる。

【0020】

請求項 6 に記載の発明は、電子機器と、請求項 3 に記載のカード型デバイスとが接続されてなる認証システムであって、前記電子機器は、前記カード型デバイスから送信される暗号化された指紋データを前記公開復号鍵により復号化し、復号化された指紋データと予め登録された指紋データとの一致を照合し、両指紋データが一致しない判断した場合、当該電子機器の動作を制限する制御部を備えたことを特徴とする。

【0021】

請求項 6 に記載の発明によれば、カード型デバイスにより暗号化された指紋データは、この秘密暗号鍵と対となる公開復号鍵に基づいて復号化可能な電子機器でしか指紋データを照合することができないので、よりセキュリティを向上することができる。

【0022】

【発明の実施の形態】

以下、図面を参照して本発明に係る第 1 の実施の形態～第 4 の実施の形態を説明する。

【0023】

〔第 1 の実施の形態〕

本発明に係る第 1 の実施の形態を説明する。

まず、構成を説明する。図 1 (a)、(b)、(c) に本実施の形態のカード型デバイスの外観構成例を示す。カード型デバイス 1 は、所定記憶容量の記憶媒体 (図示略) を有し、電子機器に設けられるカード・スロットに挿入されて使用されるものであり、例えば、PC カード、CF カード、MMC カード、SD カード、メモリスティック (登録商標) 等の規格化されたメモリカードを挙げることができる。

【0024】

カード型デバイス 1 の筐体 10 は、カード・スロットの一端部 11 には指紋読取部 2 が設けられ、他端部 12 の背面 12a には電子機器と電氣的に接続するための接続端子 13 が設けられている。また、カード型デバイス 1 は、その筐体 10 の他端部 12 側はカード・スロットに挿入される挿入部となっており、指紋読取部 2 を設けた一端部 11 はカード・スロットから露出するようになっている。

【0025】

図 2 に示すようにカード型デバイス 1 は、その機能的構成として、指紋読取部 2 および接続端子 13 の他に、信号処理部 14、メモリ 15、制御部 16、入出力 I/F 部 17 を備えている。これら各構成要素はバス 18 で接続されている。

【0026】

指紋読取部 2 は、図 3 に示すように、回転ローラ 21、光源 22、セルフオックレンズアレイ 23、基板 24、一次元指紋読取センサ 25 を含み、回転ローラ 21 の外周面 21a の一部が筐体の一端面 11a に設けられたスリット 11b から外部に突出している。

【0027】

回転ローラ 21 は円筒状を呈しており、アクリル樹脂、ポリカーボネイト、ホウケイ酸ガラス、石英ガラス等の透光性材料から構成される。スリット 11b から露出した回転ローラ 21 の外周面 21a に指 100 を圧接させて、その状態で指 100 を所定の方向に移動させると、回転ローラ 21 が回転する。

【0028】

回転ローラ 21 には指紋読取部 2 と制御部 16 との接続を ON/OFF するマ

マイクロスイッチ 19 (図 2 参照) と、回転ローラ 21 が所定角度回転する毎にパルス信号を発生して制御部 16 に出力するロータリーエンコーダ (図示略) が設けられている。マイクロスイッチ 19 は回転ローラ 21 の外周面 21a に指 100 が圧接されると ON になり、指が離されると OFF になる。

【0029】

なお、ロータリーエンコーダの代わりに、回転ローラ 21 の外周面 21a に回転量検出のための所定の印刷パターンを印刷しておき、そのパターンを読み取って制御部 16 にパルス信号を出力する回転検知センサを設けてもよい。

【0030】

図 2 および図 3 に示すように、回転ローラ 21 は中空に形成されており、その内部に光源 22、セルフオックレンズアレイ 23、基板 24、一次元指紋読取センサ 25 及びこれらの部品を保持するホルダ 26 が設けられている。ホルダ 26 は、回転ローラ 21 の一方の端又は両端から延出して筐体 10 に固定されており、回転ローラ 21 が回転してもホルダ 26 は回転しない状態に筐体 10 に支持されている。

【0031】

光源 22 は、スリット 11b に向けて光を発することで回転ローラ 21 の外周面 21a に当接した指 100 に指紋読取光 L_0 を照射するものであり、LED、有機 EL、無機 EL 及び蛍光管等といった自発光素子から構成される。

【0032】

セルフオックレンズアレイ 23 は、回転ローラ 21 の軸心に対して直交する中心軸を有する複数のセルフオックレンズを回転ローラ 21 の軸心に平行な列を成すように配列したものであり、回転ローラ 21 の外周面 21a に当接する指 100 の一次元像を一次元指紋読取センサ 25 に結像させるものである。セルフオックレンズアレイ 23 の光軸は、回転ローラ 21 の軸心に対して直交し、セルフオックレンズアレイ 23 の入射面 23a はスリット 11b に指向している。

【0033】

なお、セルフオックレンズは円柱状のロッドレンズであり、中心軸から周面にかけて放物線状の屈折率分布を有し、中心軸において屈折率が最も高く、周面に

において屈折率が最も低い自己収束型のレンズである。それぞれのセルフオックレンズは球面レンズと光学的にはほぼ等価な作用を有し、これら全てのセルフオックレンズは互いに光学的に等価な性質を有している。

【0034】

セルフオックレンズアレイ 23 が一次元指紋読取センサ 25 の受光面 25a に結像する指 100 の一次元像は、回転ローラ 21 の外周面 21a に当接された指 100 の一次元像と向きが等しく（反転されず）、等倍になる。

【0035】

基板 24 は、一次元指紋読取センサ 25 を表面に実装するとともに、信号処理部 14 と制御部 16 と信号の送受を行うための配線が施されている。

【0036】

一次元指紋読取センサ 25 は、リニア型 CCD イメージセンサ、リニア型 CMOS イメージセンサ等の光電変換素子で構成され、その受光面 25a はスリット 11b に対向するように、回転ローラ 21 の軸心に沿って平行に設けられている。セルフオックレンズアレイ 23 等により受光面 25a に結像された指紋の一次元像を電気信号としての一次元指紋信号に変換する。

【0037】

信号処理部 14 は、アナログ信号である一次元指紋信号をデジタル信号に変換して一次元指紋データを生成し、制御部 16 を介してメモリ 15 に出力する。

【0038】

制御部 16 は、CPU (Central Processing Unit)、RAM (Random Access Memory)、ROM (Read Only Memory) 等を備え、RAM または ROM に記憶された指紋読取プログラム等の指定されたプログラムを RAM の所定領域に展開し、これらのプログラムに基づく指紋読取処理等の各種処理を実行する。

【0039】

指紋読取処理はマイクロスイッチ 19 が ON することにより開始される。ユーザが回転ローラ 21 の外周面 21a に指 100 を圧接させた状態で一方向に移動させると、回転ローラ 21 が回転する。このとき、マイクロスイッチ 19 は ON になり、ロータリーエンコーダから回転ローラ 21 の所定角度回転する毎にパル

ス信号が発生される。光源 22 は指 100 に対して指紋読取光 L_0 を照射する。指 100 に反射した光 L はセルフオックレンズアレイ 23 等により一次元指紋読取センサ 25 の受光面 25a に集光される。一次元指紋読取センサ 25 は、パルス信号に同期して一次元指紋信号を生成し、信号処理部 14 に出力する。信号処理部 14 では、パルス信号に同期して順次入力される一次元指紋信号を A/D 変換して一次元指紋データを生成し、メモリ 15 に出力する。制御部 16 は、メモリ 15 に格納された一次元指紋データから、回転ローラ 21 の回転方向に基づいて指紋の二次元像としての指紋データを合成する。

【0040】

生成された指紋データは、入出力 I/F 部 17、接続端子 13 を介して電子機器に送信される。なお、入出力 I/F 部 17 は、電子機器との間で指紋データを含む種々のデータを所定のデータ伝送方式に従って伝送するものである。

【0041】

次に、図 4～図 8 を参照して、上記カード型デバイス 1 が装着される電子機器 3 (3a～3e) について説明する。電子機器 3 は、カード型デバイス 1 が装着されることにより指紋に基づくユーザの認証を行うことができる。

【0042】

図 4 に示すように、電子機器 3 は、カード・スロット 31、操作入力部 32、表示部 33、音声入出力部 40、移動体通信部 50、本体機能制御部 60 等を備え、これらはバス 34 により互いに接続される。電子機器 3 は、外部との無線通信機能、住所録機能、スケジュール管理機能等各種の機能を備えるもので、これらの機能の一部または全てをユーザの認証結果に基づいて制限することができる。

【0043】

また、これらの電子機器 3 は、カード型デバイス 1 を装着することにより、WEB サイトへのアクセス認証やインターネット等のネットワークを介して行われる電子商標取引等における電子決済の際の本人認証装置として使用することもできる。

【0044】

このような電子機器 3 として、例えば、図 5 (a)、(b) に示す携帯電話 3 a、3 b、図 6 に示す折り畳み式携帯電話 3 c、図 7 に示す P D A 等の携帯型情報機器 3 d、図 8 に示す腕時計等の身体装着型電子機器 3 e 等を挙げることができる。

【0045】

図 5～図 8 に示すように、これらの電子機器 3 a～3 e に設けられるカード・スロット 3 1 の位置は限定されるものではなく、カード型デバイス 1 を装着させたとき、指紋読取部 2 の回転ローラ 2 1 を指で圧接しながら回転させることができるようになっている。

【0046】

カード・スロット 3 1 は接続コネクタ 3 1 a を備え、このカード・スロット 3 1 にカード型デバイス 1 が挿入されて、接続端子 1 3 と接続されることにより、カード型デバイス 1 と電子機器 3 とが互いに電氣的に接続される。

【0047】

操作入力部 3 2 は、テンキー、各種機能スイッチ等を備え、そのキー操作による押下信号を C P U 6 1 に出力する。

【0048】

表示部 3 3 は、L C D (Liquid Crystal Display) 等からなる表示画面を備え、C P U 6 1 から入力される表示情報に基づく表示を行う。

【0049】

音声入出力部 4 0 は、マイク 4 1 と、スピーカ 4 2 と、音声コーデック部 4 3 とを備えて構成される。音声コーデック部 4 3 はマイク 4 1 から入力される音声信号 (アナログ信号) を A/D 変換器によりデジタル音声信号に変換し、移動体通信部 5 0 に出力する。また移動体通信部 5 0 を介して外部受信された音声信号 (デジタル信号) を復号し、D/A 変換器によりアナログ音声信号に変換して、スピーカ 4 2 に出力する。

【0050】

移動体通信部 5 0 は、無線基地局 (図示せず) との間で着信・発信等に係る無線信号の送受信を行うアンテナ 5 1、R F/送受信部 5 2、加入者 I D/端末 I

D記憶部53、通信制御部54等を備え、CPU61から入力される指示に従って、通信制御部54が無線基地局との間でIMT-2000準拠の通信方式（例えば、W-CDMAやcdma2000）に対応する携帯電話用の通信プロトコルを実行し、この通信方式で設定される通信チャネルにより、送受話音声の送受信やデータ通信を実行する。

【0051】

本体機能制御部60は、CPU61、RAM62、プログラムメモリ63、データメモリ64、入出力I/F部65を備え、CPU61において、RAM62の所定領域を作業領域としてプログラムメモリ63に記憶されている各種制御プログラムに従い、各部に制御信号を送って電子機器3の動作全般を制御する。

【0052】

プログラムメモリ63は、指紋照合プログラム63a、声紋照合プログラム63bを含むユーザ認証プログラム63cを格納している。

ここで、本実施の形態においては、制御部はCPU61において、この指紋照合プログラムに基づく指紋照合処理によりユーザ認証処理を実行する際に、マイクから入力されるユーザの音声（声紋）に基づく声紋照合処理とを併用することもできる。

【0053】

データメモリ64は、予め登録された正規のユーザの指紋データが格納された指紋データ格納領域64aと、同じく正規のユーザの声紋データが格納された声紋データ格納領域64bを有している。

【0054】

次に、ユーザ認証処理について説明する。ユーザがカード型デバイス1をカード・スロット31に挿入すると電子機器3の本体機能制御部60はユーザ認証プログラムを起動し、指紋照合処理を実行する。

【0055】

指紋照合処理では、まず、表示部33にユーザに対して回転ローラ21に指100を圧接させて一方向に移動させるように促す表示がされる。なお、このとき、スピーカ42によりその旨を音声報知することとしてもよい。

【0056】

ユーザが回転ローラ 21 を指 100 で回転させると、上記したとおり、カード型デバイス 1 の制御部 16 による指紋読取処理が実行され、互いの入出力 I/F 部 17、65 を介してカード型デバイス 1 から指紋データが電子機器 3 に送信される。

【0057】

指紋データを受信すると、電子機器 3 側の本体機能制御部 60 は、ユーザの指紋データと、データメモリ 64 に登録された指紋データとを照合し、両指紋データが一致するか否かを判断する。なお、このとき、それぞれの指紋データから特徴パターンを抽出して、その特徴パターンに基づいて両者を照合してもよい。また、回転ローラ 21 に圧接された指 100 の位置や押し付ける強さ等によって指紋データにずれが生じることが想定されるので、両者の照合率 A を求め、求めた照合率 A が予め定めた基準値（例えば、85% など）以上であれば両指紋データが一致すると判断してもよい。

【0058】

照合の結果、両指紋データが一致すると判断されると、表示部 33 にその結果を表示させるとともに、声紋照合処理を開始する。

【0059】

声紋照合処理では、マイク 41 から採取されたユーザの声紋と、データメモリ 64 の声紋データ格納領域 64b に登録された登録声紋データとが照合され、両声紋データが一致すると判断されると、ユーザが予め登録されている正規のユーザであることが認証される。

【0060】

このユーザ認証処理によって、ユーザが正規のユーザであると認証されない場合、電子機器 3 の各種機能は制限されたままの状態となる。

【0061】

なお、データメモリ 64 には複数の登録者の指紋データや声紋データを格納しておくことができ、電子機器 3 はカード型デバイス 1 を装着することにより複数のユーザを認証することができる。従って、登録者毎に電子機器 3 において使用

できる機能と使用できない機能を設定することもできる。

【0062】

また、ユーザの認証結果は、所定の時間、操作入力部 32 からの操作が行われない場合、その認証結果を消去して初期状態にすることが望ましい。

【0063】

以上説明したカード型デバイス 1 によれば、一次元指紋読取センサ 25 により指紋の二次元像を得ることとしたので、この一次元指紋読取センサ 25 を実装するための面積を小さくすることができ、CF カード等の超小型のメモリカードにも指紋読取センサ設けることができる。また、二次元の指紋読取センサを設ける場合に比べて、CCD 等の指紋センサを構成する部品コストを低減することができる。これらにより、携帯電話 3a、3b、3c、PDA 3d、腕時計 3e 等の一般ユーザ向けの電子機器 3 に容易に指紋認証機能を拡張させることができる。

【0064】

さらに、一次元指紋読取センサ 25 を透光性材料からなる回転ローラ 21 の内側に配しているので、指 100 を回転ローラ 21 の外周面 21a に圧接させた状態で移動させることにより、指 100 を一次元指紋読取センサ 25 に対して直交する方向に案内しながら移動させることができる。これにより、指紋読取時の指の変形やゆがみを防ぐことができる。また、ロータリーエンコーダ等により指の移動量を容易に管理することができるので、一次元指紋読取センサ 25 により一次元指紋データを取得するタイミングを制御することができる。

【0065】

また、回転ローラ 21 は、カード・スロット 31 の挿入口から突出した状態で設けられるので、回転させやすく操作性が高い。さらに、指紋読取部 2 をコンパクトに構成することができるので、カード型デバイス 1 を電子機器 3 に装着させた状態でも指紋読取部 2 がカード・スロット 31 の外部に大きく突出せず、携帯性に優れている。

【0066】

また、ユーザの認証結果に基づいて、電気機器 3 の動作を制限することができるので、電子機器 3 の不正利用、電子機器 3 に格納された個人情報等への不正ア

クセス、カード型デバイス 1 に記憶された個人情報等への不正アクセス等を防止することができる。

【0067】

なお、上記実施の形態では、カード型デバイス 1 を電子機器 3 に装着させたときに、電子機器 3 により指紋に基づくユーザ認証処理を実行させるものとしたが、これに限定されるものではない。常に電子機器 3 にカード型デバイス 1 を装着させておき、例えば、移動体通信部 50 を介してインターネット等の通信ネットワークを介して電子商取引を行うときなど、ユーザ認証が求められる場合にのみユーザ認証処理を実行させてもよい。

【0068】

また、電子機器 3 においてユーザ認証処理を行わせるものとしたが、通信ネットワークに接続された他の電子機器（例えば、サーバ）によりユーザの認証を行うものとしてもよい。

【0069】

〔第 2 の実施の形態〕

次に第 2 の実施の形態について説明する。第 2 の実施の形態では、指紋に基づくユーザ認証処理をカード型デバイス 7 において実行させることができる。なお、上記実施の形態と同様の構成については同様の符号を付してその説明を省略する。

【0070】

図 9 に第 2 の実施の形態におけるカード型デバイス 7 を示す。図 9 に示すように、カード型デバイス 7 は、指紋照合プログラムを格納したプログラムメモリ 71 と、正規ユーザの指紋データを格納したデータメモリ 72 とを有している。

【0071】

第 2 の実施の形態では、カード型デバイス 7 の制御部 16 側で指紋照合処理に基づくユーザ認証処理が実行される。この場合、制御部 16 は、プログラムメモリ 71 に格納された指紋照合プログラムに従って、指紋照合処理を実行する。指紋照合処理では、指紋読取部 2 から得た一次元指紋データに基づいて合成した指紋データと、データメモリ 72 に格納された指紋データとが照合される。両指紋

データが一致しないと判断した場合、入出力 I/F 部 17 における電子機器 3 との間のデータの授受が制限される。

【0072】

以上のカード型デバイス 7 は、電子機器 3 に接続する前に指紋に基づいてユーザを認証することが可能である。勿論、電子機器 3 にカード型デバイス 7 を装着させた状態で、指紋照合処理を実行するようにしてもよい。

【0073】

また、一次元指紋読取センサ 25 を介して取得された指紋データが、データメモリ 72 に格納された指紋データと一致しない場合は、電子機器 3 との間のデータの授受が制限されるので、カード型デバイス 7 の不正使用およびカード型デバイス 7 への不正アクセスを防止することができる。

【0074】

〔第 3 の実施の形態〕

次に、第 3 の実施の形態について説明する。なお、上記実施の形態と同様の構成については同様の符号を付してその説明を省略する。

【0075】

図 10 に示すように、第 3 の実施の形態におけるカード型デバイス 8 は、暗号化回路 81 と、秘密鍵を記憶した秘密鍵メモリ 82 とを有している。信号処理部 14、メモリ 15、制御部 16、暗号化回路 81、秘密鍵メモリ 82 は、耐タンパー性の認証チップ内に集積されている。

【0076】

耐タンパー性とは、ある程度までの物理的衝撃（不当アクセス・改竄等）に抵抗する機能をいい、外部からの不当なアクセスに対し、物理的な仕組みによってアクセスできないようにする他、分解して解析するなどがあった場合には、チップそのものが回路的に破壊されるような、偽造・変造・改竄等を防止する手段を備えたものをいう。

【0077】

暗号化回路 81 は、秘密鍵メモリ 82 に格納されたこのカード型デバイス 8 に固有の秘密暗号鍵に基づいて、制御部 16 により合成された指紋データを暗号化

して、入出力 I/F 部 17 を介して電子機器 3 に送信する。

【0078】

ここで、秘密暗号鍵とは、いわゆる公開鍵暗号化方式（PKI：Public Key Infrastructure）による暗号化・復号化を行うための鍵情報である。この秘密暗号鍵により暗号化された情報は、対応する公開復号鍵によってのみ復号化が可能である。

【0079】

従って、本実施の形態によれば、暗号化回路 81 により秘密暗号鍵により暗号化された指紋データを電子機器 3 または電子機器 3 を介して接続されるネットワーク上のサーバ等へ送信するので、電子機器 3 またはネットワーク上のサーバ等は、この秘密暗号鍵と対となる公開復号鍵を有する場合しか指紋データを復号化することができない。よって、指紋データの悪用を防止することができ、セキュリティをより高めることができる。

【0080】

〔第 4 の実施の形態〕

次に、第 4 の実施の形態について説明する。なお、上記実施の形態と同様の構成については同様の符号を付してその説明を省略する。

【0081】

図 11 に、第 4 の実施の形態におけるカード型デバイス 9 としての USB 接続携帯型フラッシュメモリの外観構成例を（a）、（b）、（c）に示す。図 11（a）、（b）、（c）に示した USB 接続携帯型フラッシュメモリは、それぞれ筐体 90 の他端部 91 に USB 端子 92 を備え、筐体 90 の端面に指紋読取部 2 を備え、回転ローラ 21 が端面から突出してもうけられている。また、内部にはフラッシュメモリ Flash EPROM（Erasable Programmable Read Only Memory）を収容しており、外部メモリ装置として使用することができる。

【0082】

これらのカード型デバイス 9 は、USB 規格に基づいたシリアルインターフェース回路を備えた電子機器（例えば、PDA、パーソナルコンピュータ）等に着脱することにより互いにデータの授受を行うことができる。

【0083】

次に、カード型デバイス 9 の機能的構成を説明する。図 12 に示すように、カード型デバイス 9 は、USB 接続端子 92 と、USB 入出力 I/F 回路 93 と、暗号化回路 81 と、秘密鍵を記憶した秘密鍵メモリ 82 と、信号処理部 14、メモリ 15、制御部 16、指紋読取部 2 を有している。第 3 の実施の形態と同様に、信号処理部 14、メモリ 15、制御部 16、暗号化回路 81、秘密鍵メモリ 82 は耐タンパー性の認証チップに集積されている。

【0084】

このカード型デバイス 9 は、公開鍵暗号方式に基づく電子証明書、パスワード等をフラッシュメモリに格納しておき、USB 端子 92 を介して接続された電子機器または電子機器を介してネットワーク上にトークン (Token) と呼ばれる特殊なデータで表現して送出するものである。このとき、指紋読取部 2 より読み取られた指紋に基づくユーザ認証が完了しない限り、電子証明書を電子機器 3 に送出できないように制御される。

【0085】

ここで、指紋データの照合は第一の実施の形態と同様にカード型デバイス 9 が接続された電子機器側で行うものとしてもよいし、第二の実施の形態と同様にカード型デバイス 9 側で行うものとしてもよいし、ネットワークで接続された認証用のサーバで行うものとしてもよい。

【0086】

また、指紋データの照合をネットワーク上の認証用のサーバで行うものとした場合、指紋データを電子機器に設けられる通信部を介して認証用のサーバに送信する際に、暗号化回路により指紋データを秘密暗号鍵に基づいて暗号化して送信してもよい。

【0087】

これにより、電子商取引等のユーザ認証が求められる場面等で、指紋読取部 2 により読み取られた指紋に基づくユーザ認証が完了しない限り、個人情報である電子証明書を使用することができないので、カード型デバイス 9 に格納された電子証明書やパスワードなどの重要な個人情報の悪用を防ぎ、他者の「なりすまし

」等を防止することができる。

【0088】

【発明の効果】

請求項1に記載の発明によれば、一次元指紋読取センサにより指紋の二次元像を得ることとしたので、指紋読取センサを実装するための面積も小さくすることができ、CFカード等の超小型のメモリカードにも指紋読取センサ設けることができる。また、二次元の指紋読取センサを設ける場合に比べて、指紋センサを構成する部品コストを低減することができる。これらにより、携帯電話やPDA等の一般ユーザ向けの携帯用電子機器にも容易に指紋認証機能を拡張させることができる。

【0089】

さらに指を回転ローラに当接させた状態で回転させることにより、指を一次元指紋読取センサに対して移動させることができるので、指の変形やゆがみを防止した状態で一次元指紋読取センサに指紋を読み取らせることができ、操作性に優れている。

【0090】

請求項2に記載の発明によれば、回転ローラはカード・スロットの挿入口から露出する端面に設けられるので、カード型デバイスを装着させた状態でカード・スロットから指紋読取センサが大きく突出することがなく、携帯性に優れている。また、ユーザは、カード・スロットの挿入口に直交するように指をスライドさせればよいので、操作性に優れている。

【0091】

請求項3に記載の発明によれば、暗号化手段により指紋データを秘密暗号鍵により暗号化するので、暗号化された指紋データはこの秘密暗号鍵と対となる公開復号鍵を有するものにしか復号化することができず、指紋データの悪用を防ぎ、セキュリティをより高めることができる。

【0092】

請求項4に記載の発明によれば、カード型デバイスを電子機器に接続する前に指紋に基づいてユーザを認証することができる。また、一次元指紋読取センサを介

して取得された指紋データが、予め登録された指紋データと一致しない場合は、電子機器との間のデータの授受が制限されるので、カード型デバイスの不正使用およびカード型デバイスへの不正アクセスを防止することができる。

【0093】

請求項5に記載の発明によれば、電子機器はカード型デバイスから送信される指紋データと、予め登録された指紋データとを照合し、両指紋データが一致しないと判断した場合、制御部は電子機器の動作を制限するので、電子機器およびカード型デバイスの不正使用およびカード型デバイスへの不正アクセスを防止することができる。

【0094】

請求項6に記載の発明によれば、カード型デバイスにより暗号化された指紋データは、この秘密暗号鍵と対となる公開復号鍵に基づいて復号化可能な電子機器でしか指紋データを照合することができないので、よりセキュリティを向上することができる。

【図面の簡単な説明】

【図1】

本発明を適用した第1の実施の形態のカード型デバイスの外観構成例を示した(a)正面図、(b)側面図、(c)背面図である。

【図2】

本発明を適用した第1の実施の形態のカード型デバイスの機能的構成を示したブロック図である。

【図3】

図2に示す指紋読取部2の構成例を示した側面図である。

【図4】

本発明を適用した第1の実施の形態の電子機器の機能的構成を示したブロック図である。

【図5】

図4に示す電子機器の外観構成例(a)、(b)を示した図である。

【図6】

図 4 に示す電子機器の外観構成例を示した図である。

【図 7】

図 4 に示す電子機器の外観構成例を示した図である。

【図 8】

図 4 に示す電子機器の外観構成例を示した図である。

【図 9】

本発明を適用した第 2 の実施の形態のカード型デバイスの機能的構成を示した図である。

【図 10】

本発明を適用した第 3 の実施の形態のカード型デバイスの機能的構成を示した図である。

【図 11】

本発明を適用した第 4 の実施の形態のカード型デバイスの外観構成例を示した図である。

【図 12】

図 11 (a) に示すカード型デバイスの機能的構成を示した図である。

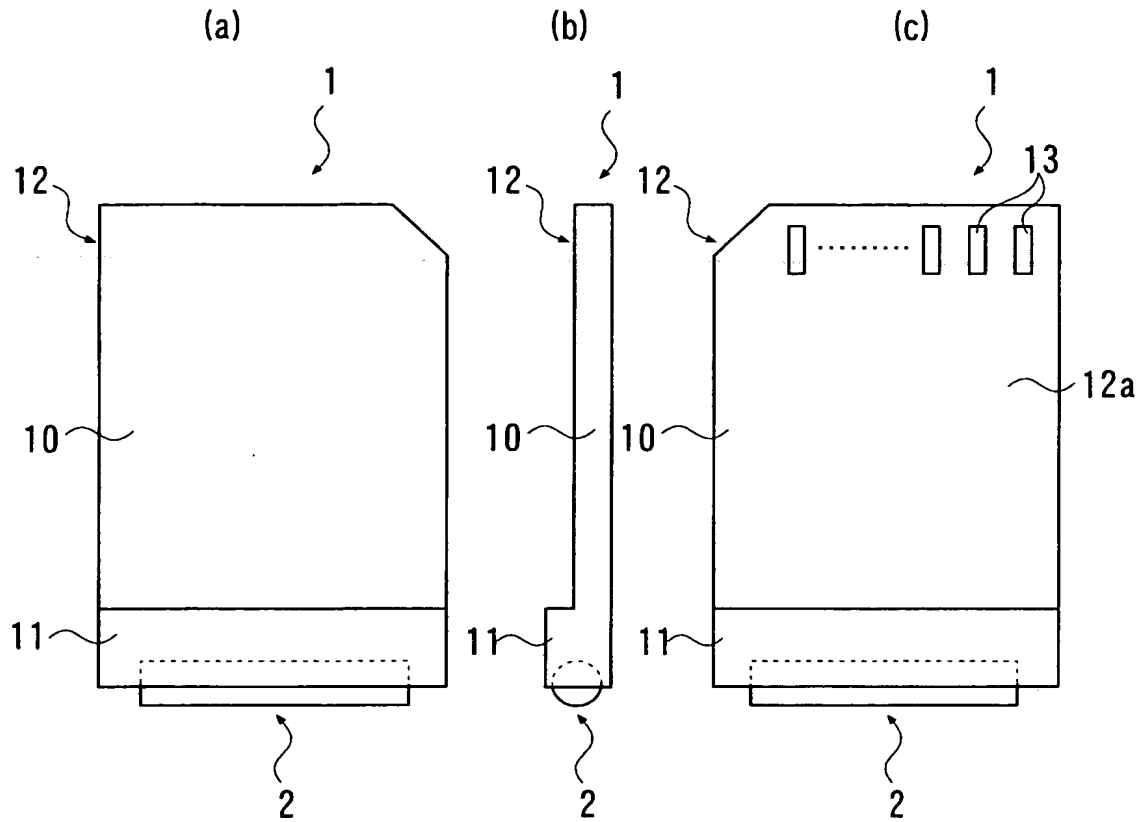
【符号の説明】

- 1 カード型デバイス
- 10 筐体
- 11a 一端面 (端面)
- 13 接続端子
- 14 信号処理部
- 15 メモリ
- 16 制御部
- 2 指紋読取部
- 21 光源
- 21 回転ローラ
- 21a 外周面
- 22 光源

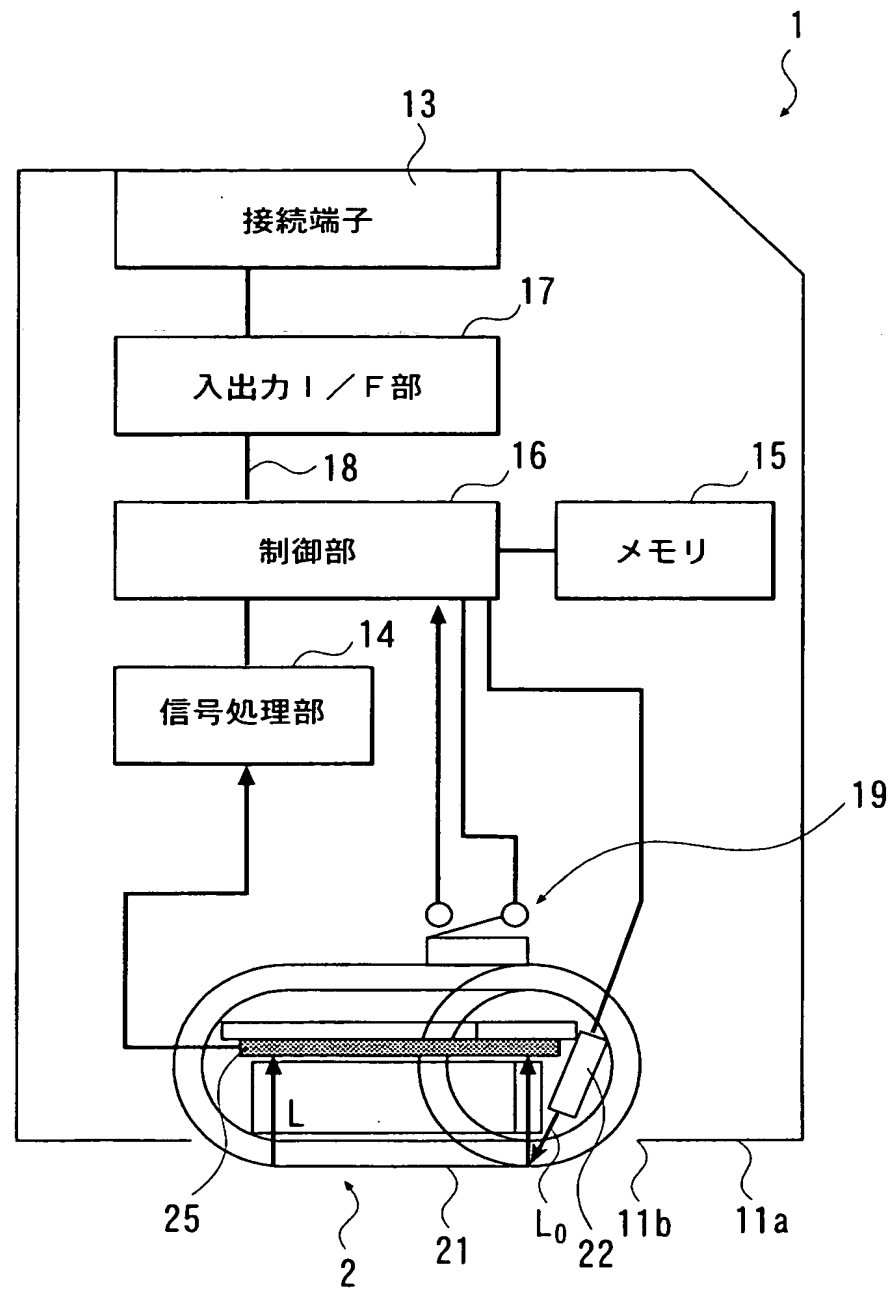
- 23 セルフォックレンズアレイ
- 24 基板
- 25 一次元指紋読取センサ
- 3 電子機器
- 31 カード・スロット
- 31a 接続コネクタ
- 60 制御部
- 63 プログラムメモリ
- 63a 指紋照合プログラム
- 63b 声紋照合プログラム
- 63c ユーザ認証プログラム
- 64 データメモリ
- 64a 指紋データ格納領域
- 64b 声紋データ格納領域
- 65 I/F部
- 7 カード型デバイス
- 71 指紋照合プログラム格納領域
- 72 指紋データ格納領域
- 8 カード型デバイス
- 81 暗号化回路
- 82 秘密鍵メモリ
- 9 カード型デバイス
- 92 USB接続端子
- 93 USB入出力I/F回路
- 100 指

【書類名】 図面

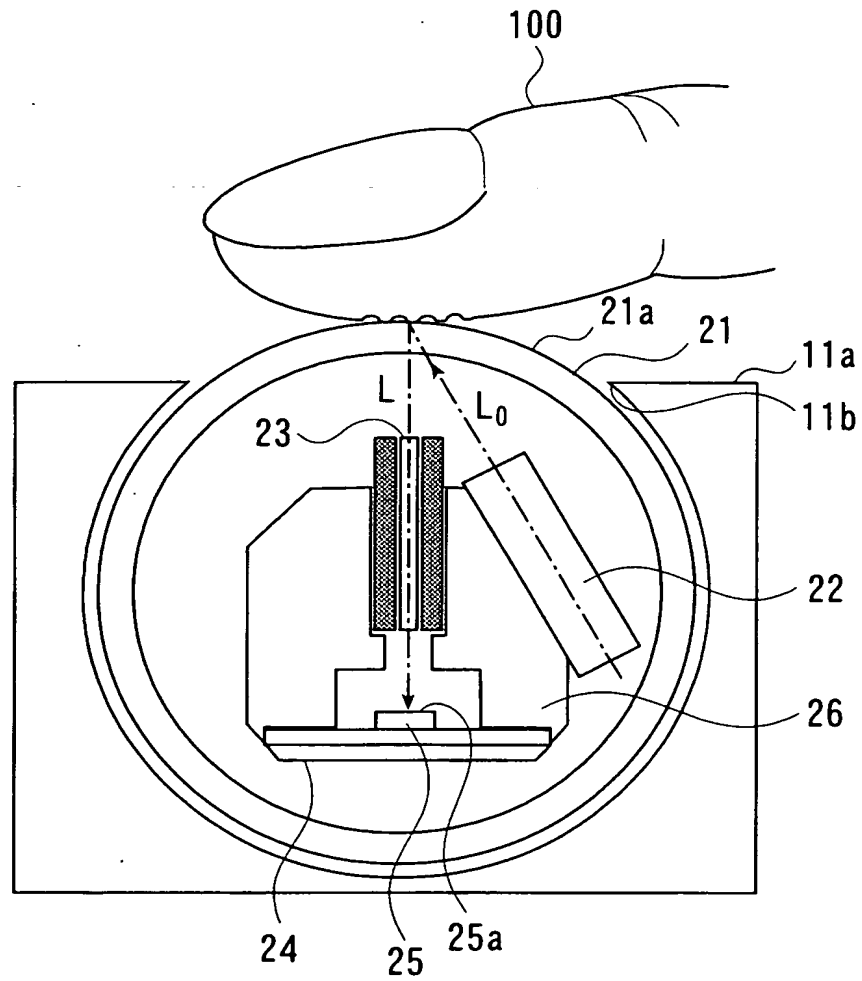
【図 1】



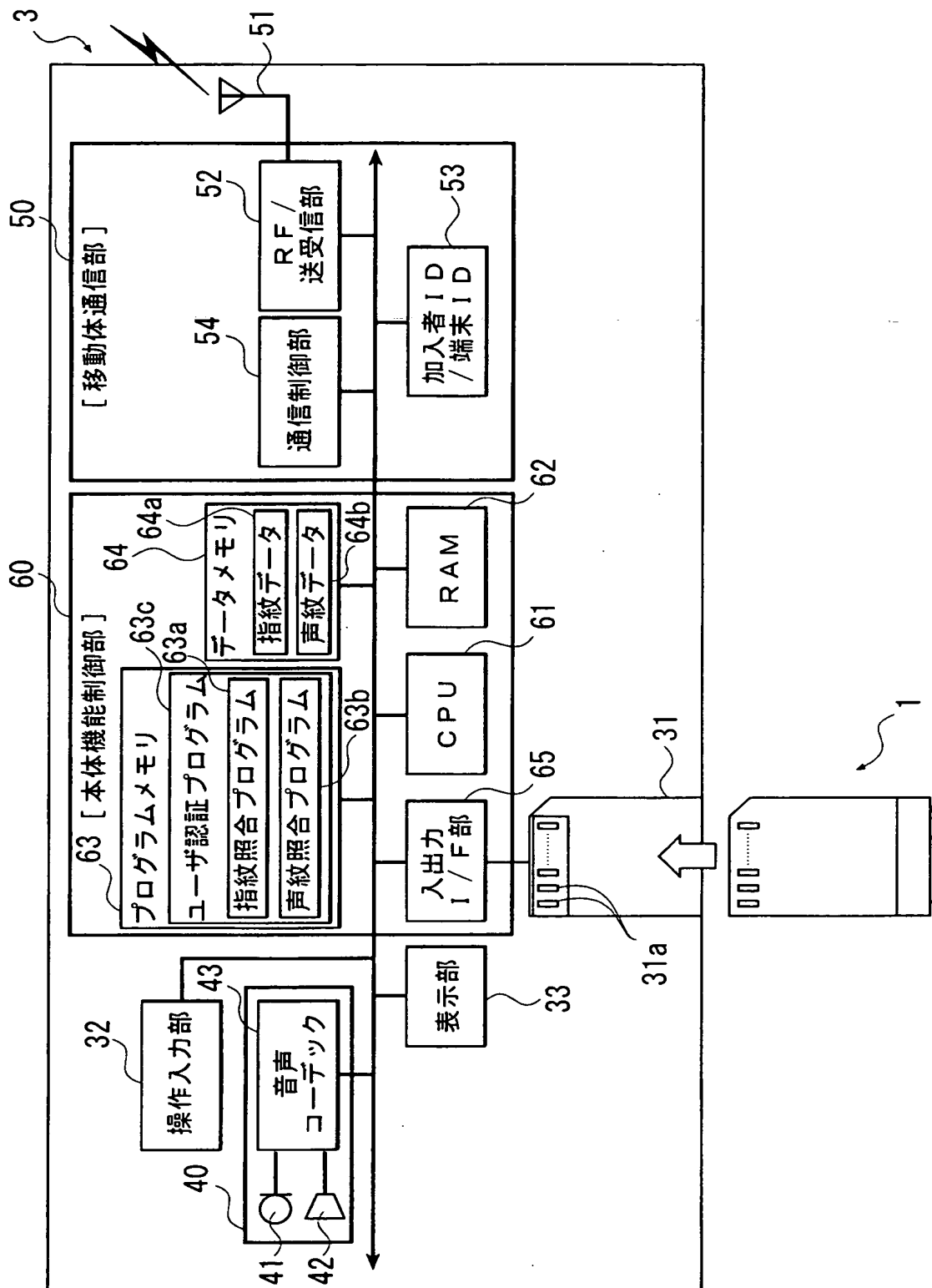
【図 2】



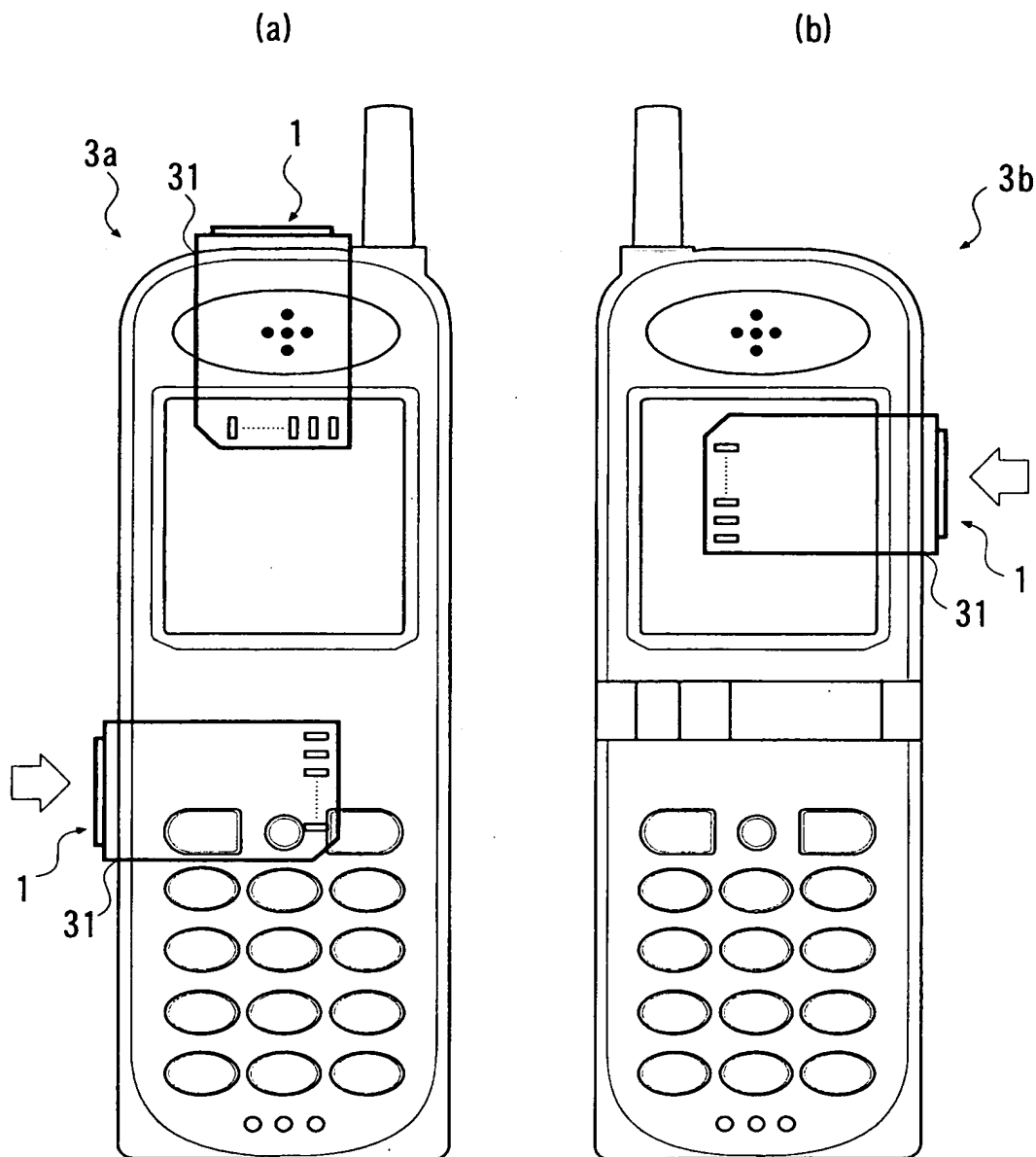
【図 3】



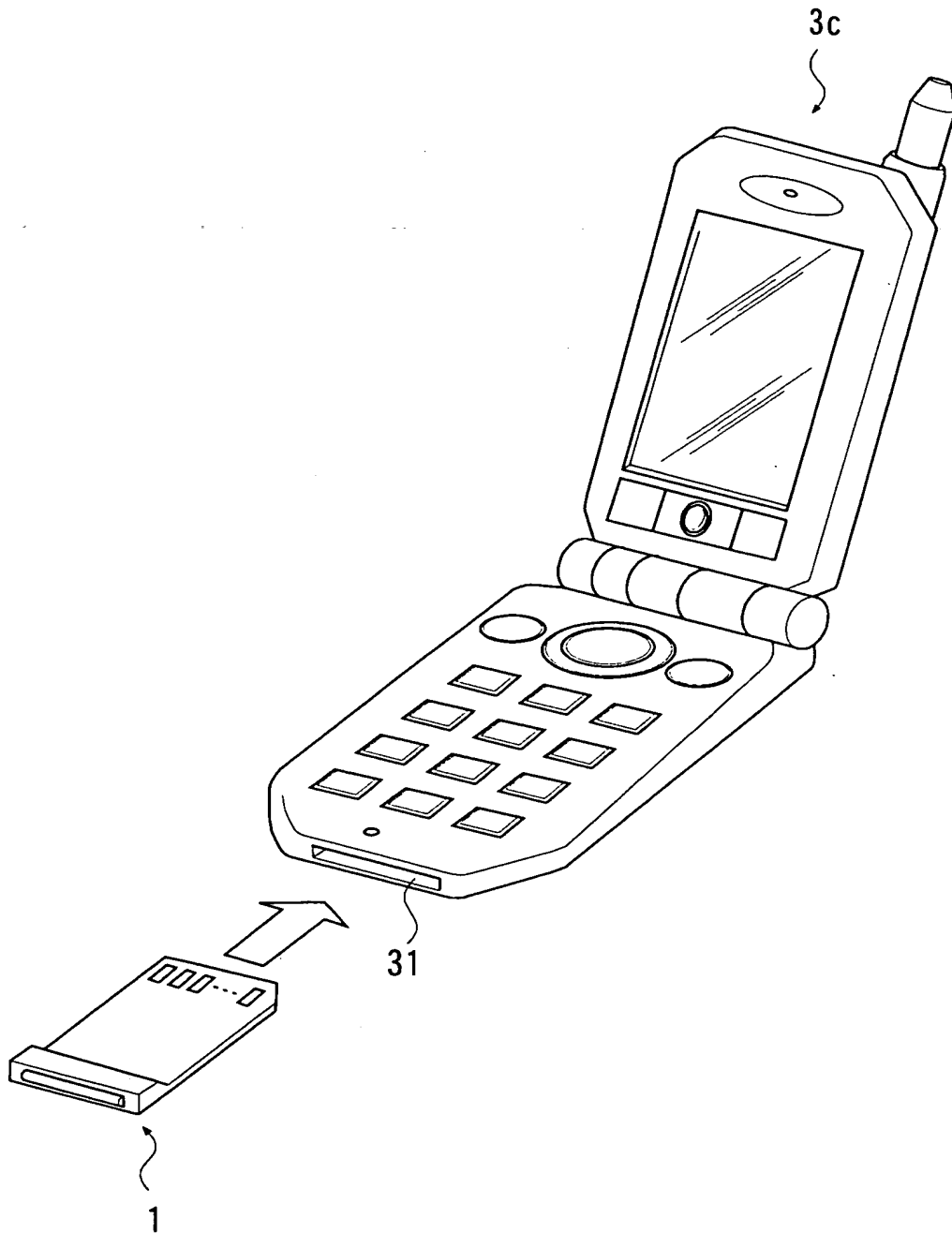
【図 4】



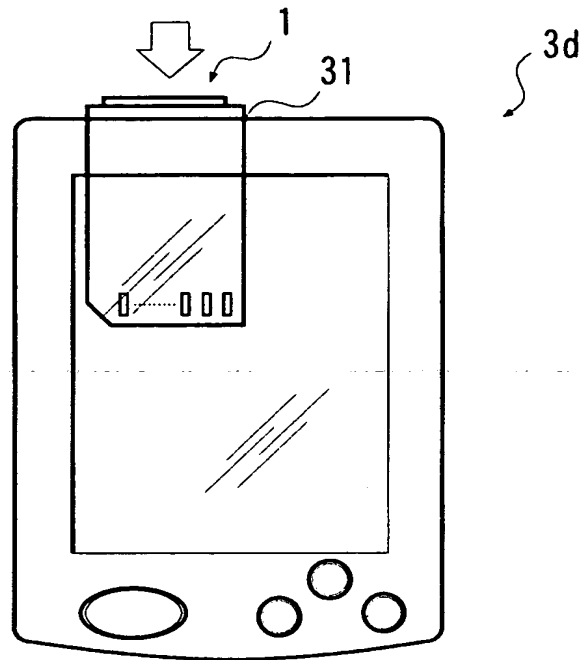
【図 5】



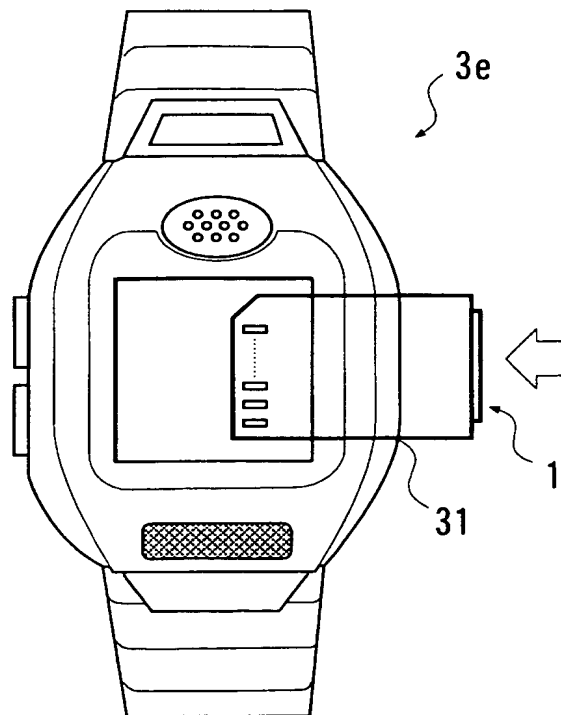
【図 6】



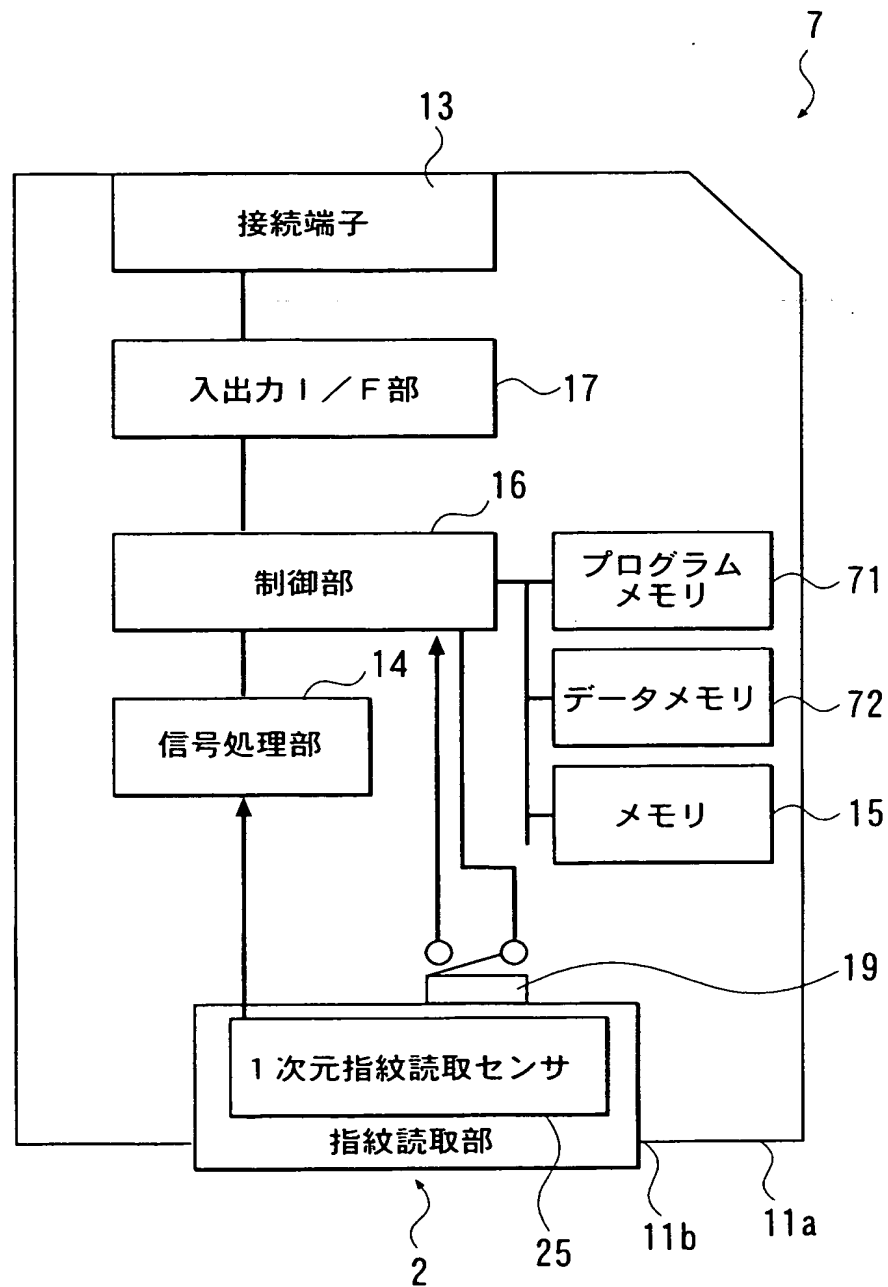
【図 7】



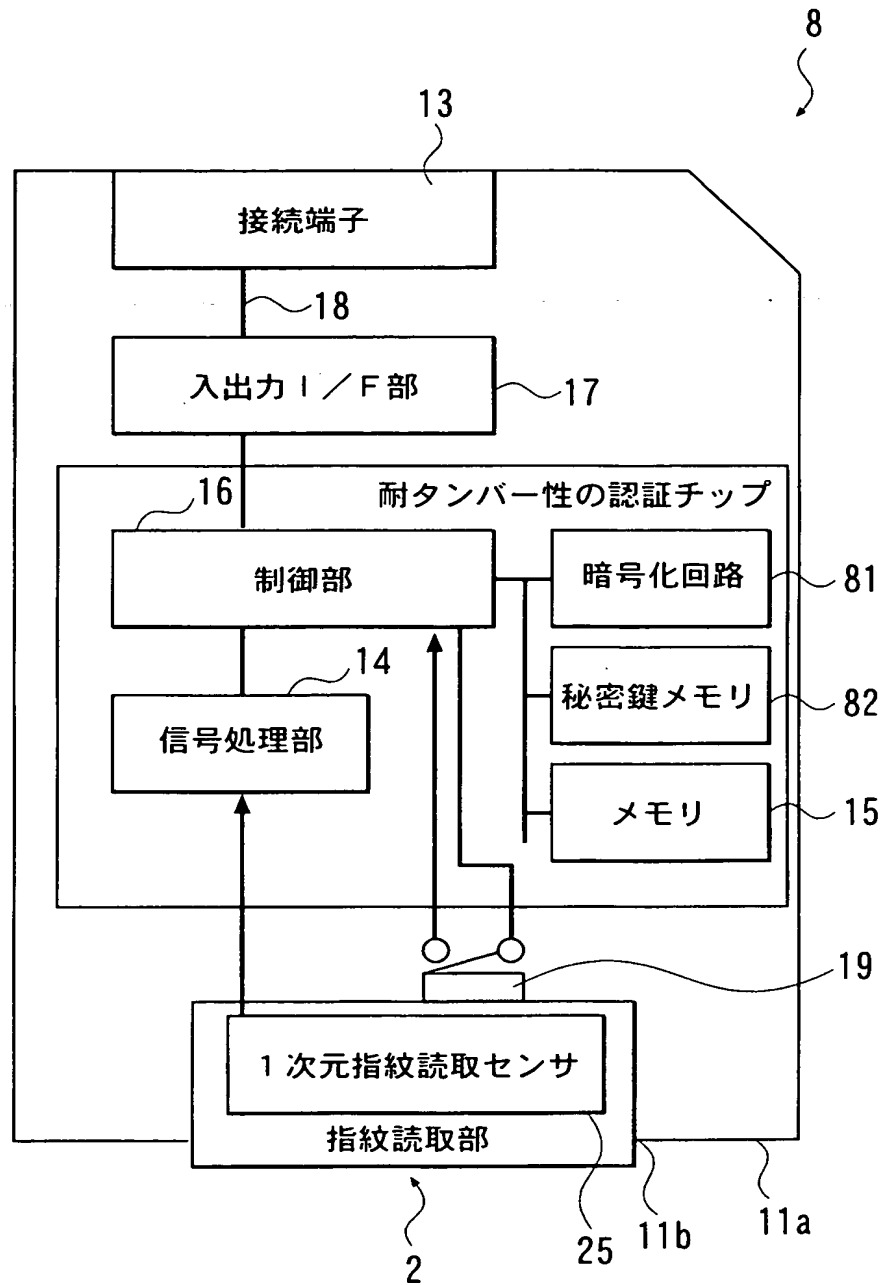
【図 8】



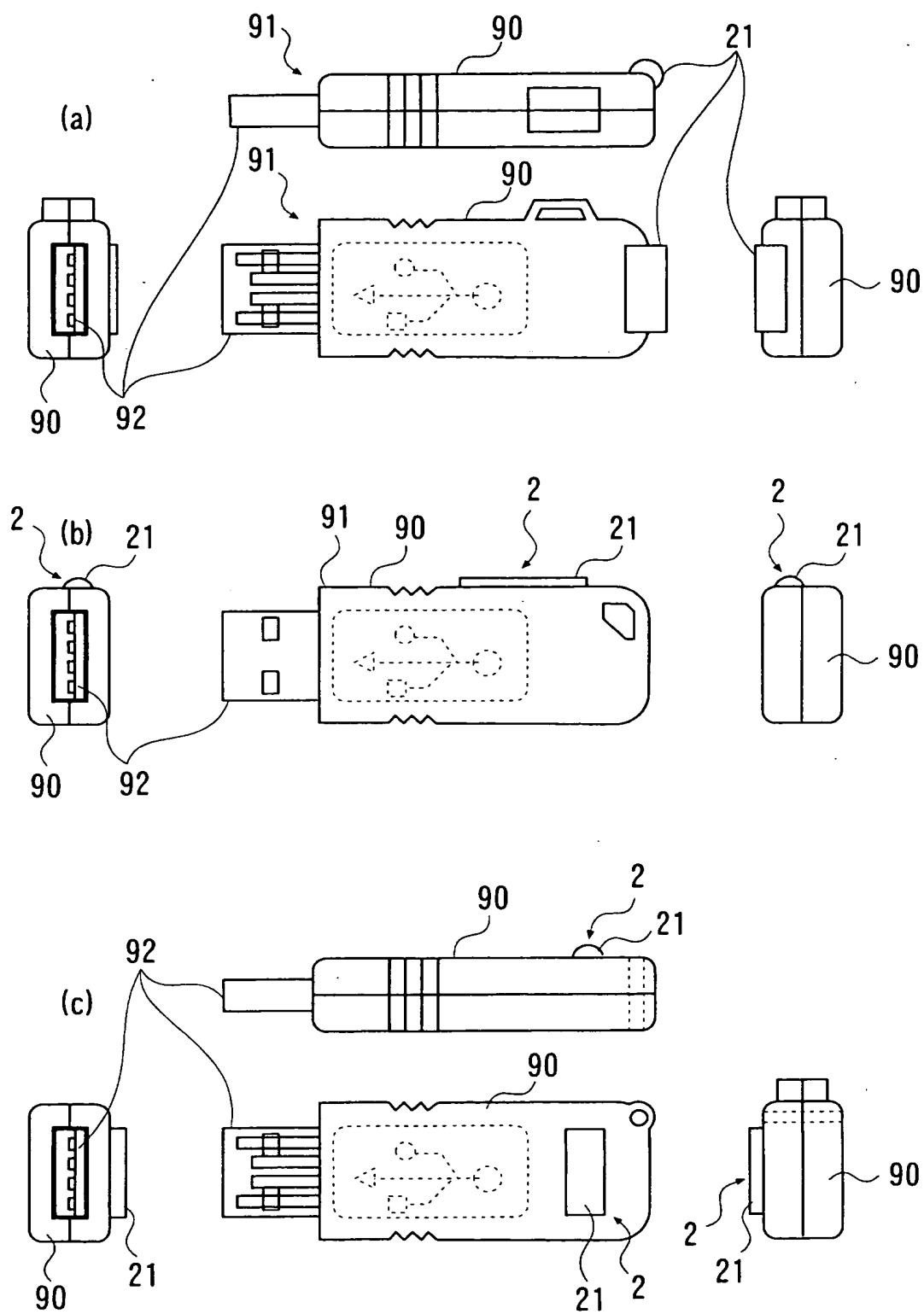
【図 9】



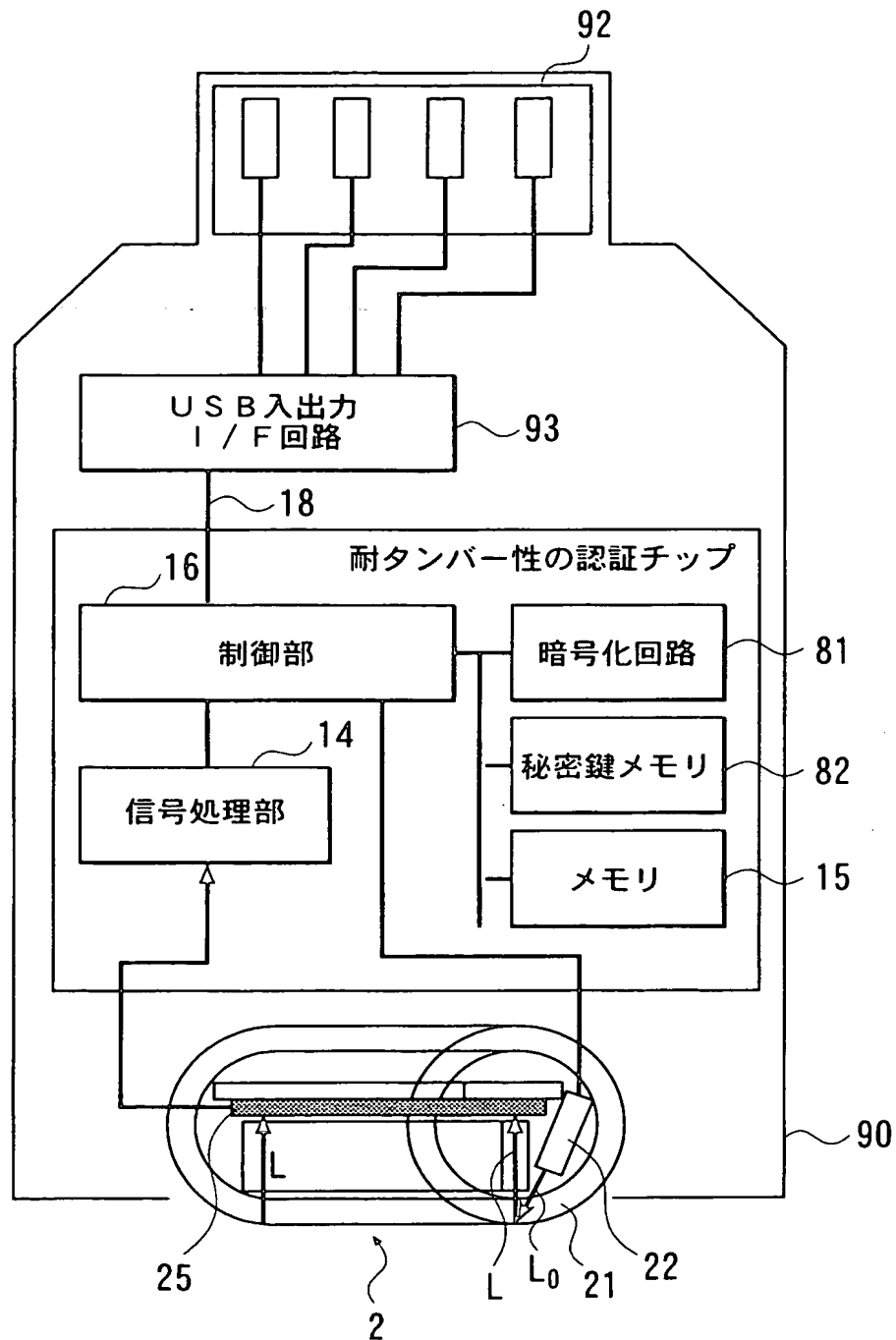
【図10】



【図 11】



【図12】



【書類名】 要約書

【要約】

【課題】 指紋読取センサを搭載した超小型のカード型デバイスおよびこのカード型デバイスを用いた認証システムを提供する。

【解決手段】 接続端子 13 を有するカード型の筐体 10 の端面に、外周面 21 a が突出するように回転ローラ 21 を設け、回転ローラ 21 の外周面 21 a に当接される指 100 の一次元指紋データを取得する一次元指紋データ取得部 25 と、回転ローラ 21 を回転させることにより、一次元指紋データ取得部 25 により位置を連続的に変えて取得される一次元指紋データから二次元像としての指紋データを合成する指紋データ合成部 16 と、電子機器 3 との間でデータの授受を行うインターフェース部 17 を設ける。

【選択図】 図 2

特願 2 0 0 2 - 3 7 4 7 2 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 1 4 4 3]

1. 変更年月日

1 9 9 8 年 1 月 9 日

[変更理由]

住所変更

住 所

東京都渋谷区本町 1 丁目 6 番 2 号

氏 名

カシオ計算機株式会社